# INTERNATIONAL CYBERSECURITY AND DIGITAL FORENSICS ACADEMY

**Assignment Title:** Malware Sample 2-UPX Packed
**Course Code:** ACI803 Malware Analysis for Cybercrime

**Student Name:** Ahtisham Tanveer

**Student ID:** 2025/ACI/9979

**Programme:** Advance Cybercrime Investigations

**Instructor Name**: Aminu Idris

**Date of Submission:** 10/08/2025

STUDENT ID CARD

AHTISHAM TANVEER
2025/ACI/9979
CYBERCRIME INVESTIGATIONS

Exp Date: **November, 2025**

## Executive Summary

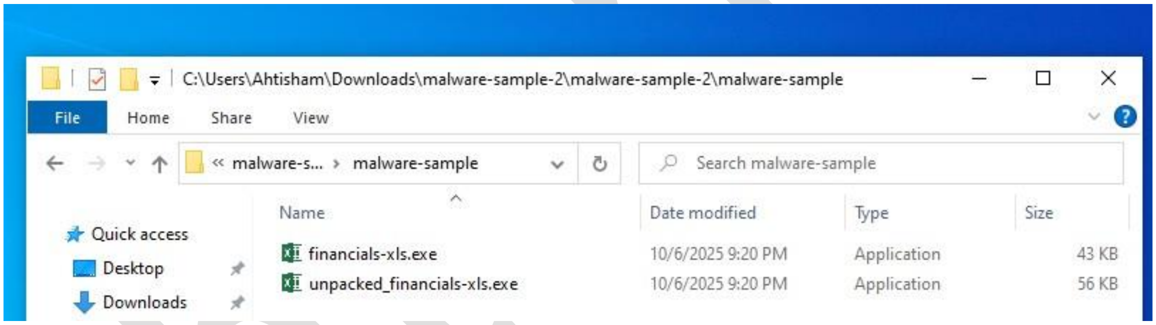
The analyzed sample, **RAT.Unknown.exe**, was obtained from the ICDFA Malware Repository and identified as a **Remote Access Trojan (RAT)**. The sample was initially packed with **UPX**, indicating an attempt to obfuscate its original code and hinder analysis.

Through systematic static analysis using tools such as **PE Studio**, **Die**, **BinText**, and **FLOSS**, followed by structural inspection using **CFF Explorer** and **PE view**, the malware was found to exhibit RAT-like capabilities including **registry-based persistence**, **keylogging**, **screen capture**, and **command-and-control (C2) communication** over HTTP.

Dynamic and behavioral enrichment was obtained via **Virus Total** and **Hybrid Analysis**, which revealed multiple network indicators, API call traces, and malicious behaviors consistent with **known RAT families**.

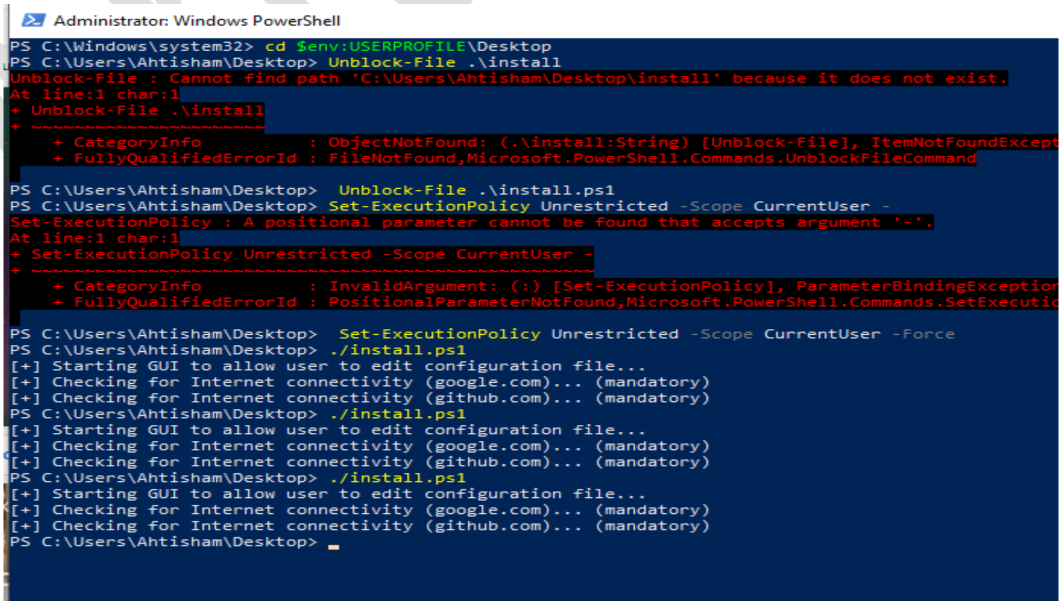
The malware leverages Windows APIs for process injection, registry modification, and credential access. The absence of a digital signature and the use of UPX packing further confirm its malicious intent.
This report provides a structured breakdown of static, structural, and behavioral findings, mapped against the **MITRE ATT&CK framework**.

## Basic File Structure:



C:\Users\Ahtisham\Downloads\malware-sample-2\malware-sample-2\malware-sample

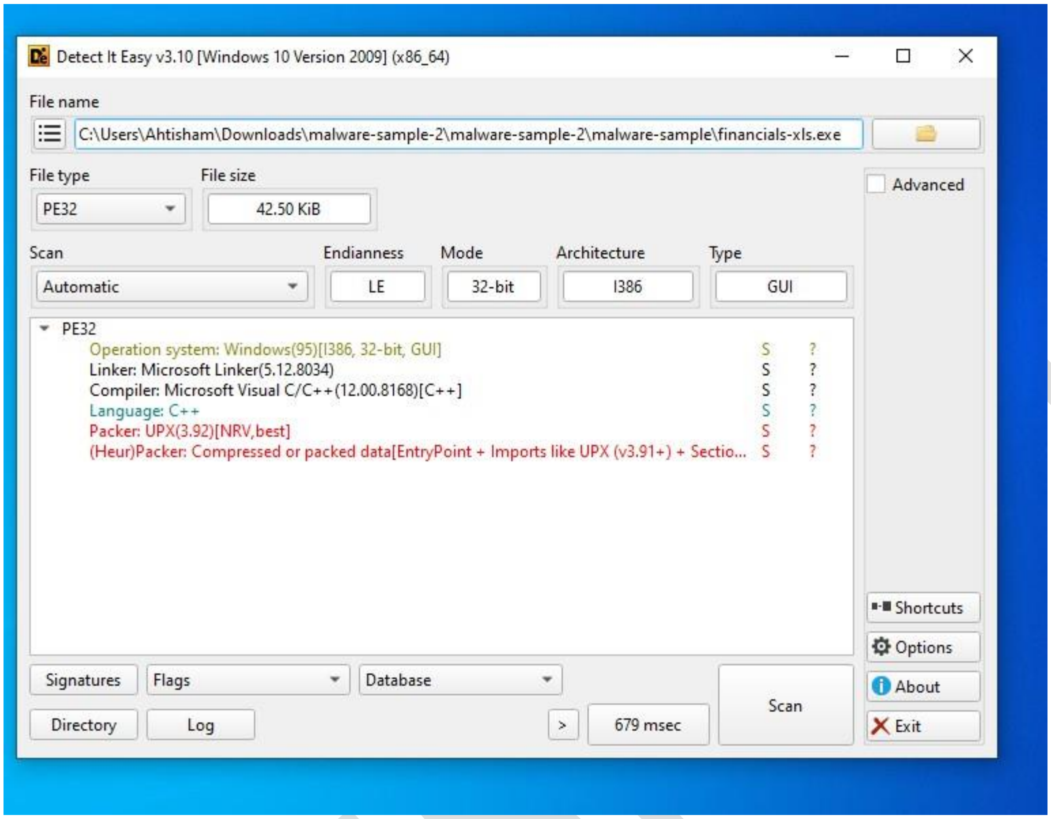
| Name | Date modified | Type | Size |
|---|---|---|---|
| financials-xls.exe | 10/6/2025 9:20 PM | Application | 43 KB |
| unpacked_financials-xls.exe | 10/6/2025 9:20 PM | Application | 56 KB |



Administrator: Windows PowerShell

```
PS C:\Windows\system32> cd $env:USERPROFILE\Desktop
PS C:\Users\Ahtisham\Desktop> Unblock-File .\install
Unblock-File : Cannot find path 'C:\Users\Ahtisham\Desktop\install' because it does not exist.
At line:1 char:1
+ Unblock-File .\install
+ ~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (.\install:String) [Unblock-File], ItemNotFoundExcept
    + FullyQualifiedErrorId : FileNotFound,Microsoft.PowerShell.Commands.UnblockFileCommand

PS C:\Users\Ahtisham\Desktop>  Unblock-File .\install.ps1
PS C:\Users\Ahtisham\Desktop> Set-ExecutionPolicy Unrestricted -Scope CurrentUser -
Set-ExecutionPolicy : A positional parameter cannot be found that accepts argument '-'.
At line:1 char:1
+ Set-ExecutionPolicy Unrestricted -Scope CurrentUser -
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Set-ExecutionPolicy], ParameterBindingExceptior
    + FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.SetExecutic

PS C:\Users\Ahtisham\Desktop>  Set-ExecutionPolicy Unrestricted -Scope CurrentUser -Force
PS C:\Users\Ahtisham\Desktop> ./install.ps1
[+] Starting GUI to allow user to edit configuration file...
[+] Checking for Internet connectivity (google.com)... (mandatory)
[+] Checking for Internet connectivity (github.com)... (mandatory)
PS C:\Users\Ahtisham\Desktop> ./install.ps1
[+] Starting GUI to allow user to edit configuration file...
[+] Checking for Internet connectivity (google.com)... (mandatory)
[+] Checking for Internet connectivity (github.com)... (mandatory)
PS C:\Users\Ahtisham\Desktop> ./install.ps1
[+] Starting GUI to allow user to edit configuration file...
[+] Checking for Internet connectivity (google.com)... (mandatory)
[+] Checking for Internet connectivity (github.com)... (mandatory)
PS C:\Users\Ahtisham\Desktop> _
```

## 1. File Type Verification: TOOLS(Die)



File name: C:\Users\Ahtisham\Downloads\malware-sample-2\malware-sample-2\malware-sample\financials-xls.exe

File type: PE32

File size: 42.50 KiB

☐ Advanced

Scan: Automatic

Endianness: LE

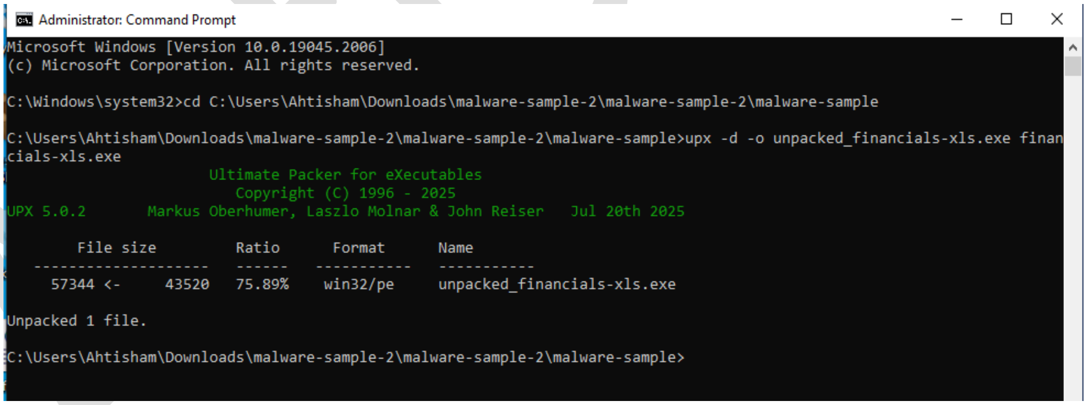
Mode: 32-bit

Architecture: I386

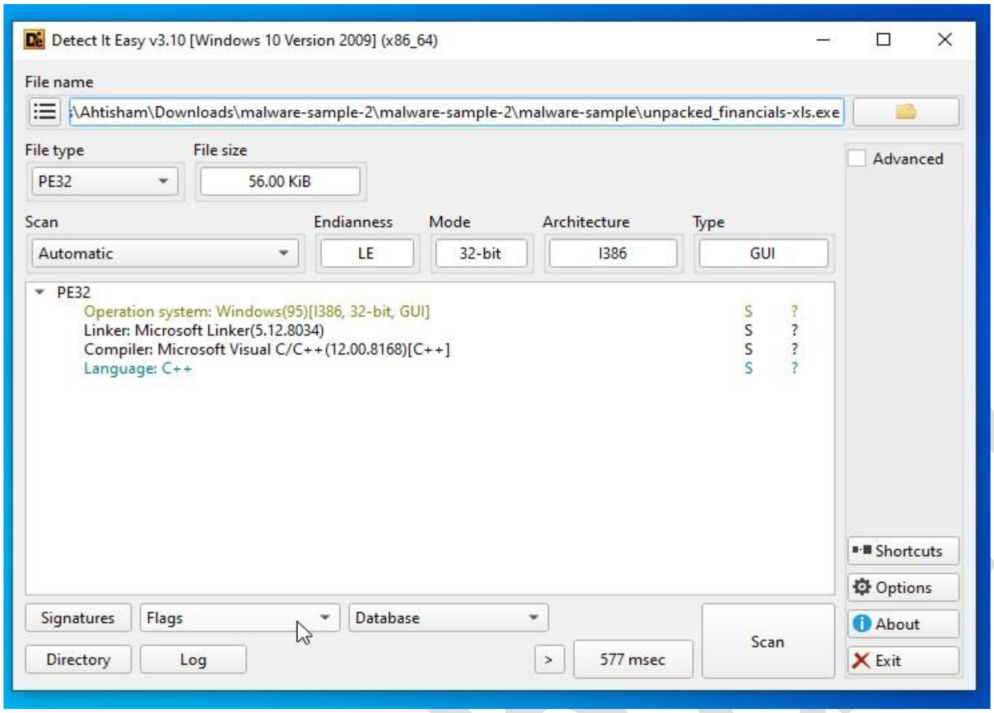
Type: GUI

```
PE32
    Operation system: Windows(95)[I386, 32-bit, GUI]                                  S    ?
    Linker: Microsoft Linker(5.12.8034)                                               S    ?
    Compiler: Microsoft Visual C/C++(12.00.8168)[C++]                                 S    ?
    Language: C++                                                                     S    ?
    Packer: UPX(3.92)[NRV,best]                                                       S    ?
    (Heur)Packer: Compressed or packed data[EntryPoint + Imports like UPX (v3.91+) + Sectio...  S    ?
```

679 msec



```
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Ahtisham\Downloads\malware-sample-2\malware-sample-2\malware-sample

C:\Users\Ahtisham\Downloads\malware-sample-2\malware-sample-2\malware-sample>upx -d -o unpacked_financials-xls.exe finan
cials-xls.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2025
UPX 5.0.2       Markus Oberhumer, Laszlo Molnar & John Reiser   Jul 20th 2025

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     57344 <-     43520   75.89%    win32/pe     unpacked_financials-xls.exe

Unpacked 1 file.

C:\Users\Ahtisham\Downloads\malware-sample-2\malware-sample-2\malware-sample>
```



Detect It Easy v3.10 [Windows 10 Version 2009] (x86_64)

File name: :\Ahtisham\Downloads\malware-sample-2\malware-sample-2\malware-sample\unpacked_financials-xls.exe

File type: PE32

File size: 56.00 KiB

Scan: Automatic

Endianness: LE

Mode: 32-bit

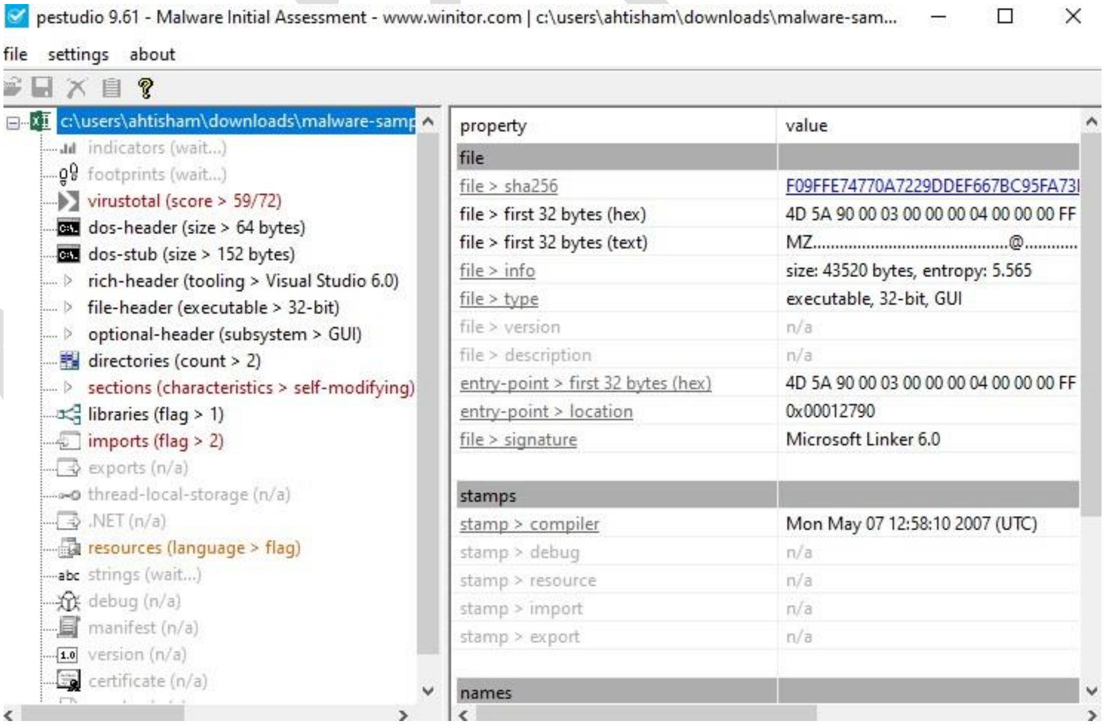
Architecture: I386

Type: GUI

```
PE32
    Operation system: Windows(95)[I386, 32-bit, GUI]      S   ?
    Linker: Microsoft Linker(5.12.8034)                   S   ?
    Compiler: Microsoft Visual C/C++(12.00.8168)[C++]     S   ?
    Language: C++                                         S   ?
```

577 msec

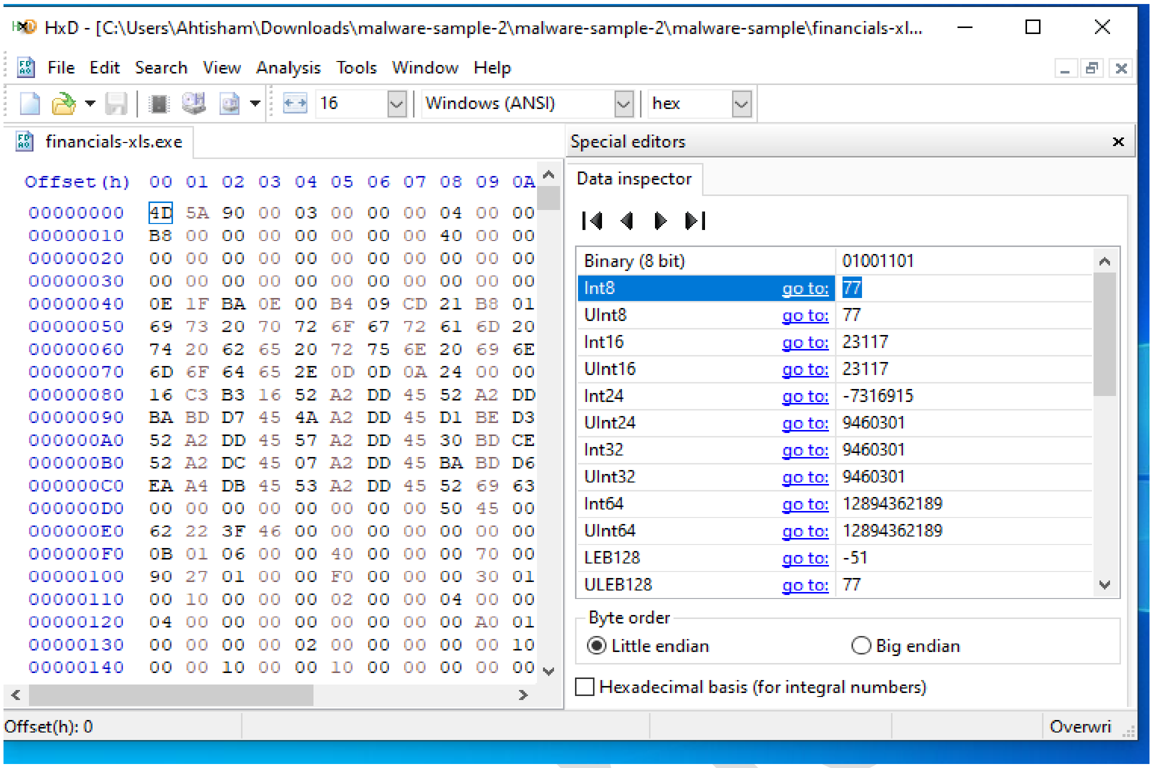
## Hashing, entropy, String Extraction and Compiler Identification: Tools(Pestudio)



pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\ahtisham\downloads\malware-sam...

```
c:\users\ahtisham\downloads\malware-samp
    indicators (wait...)
    footprints (wait...)
    virustotal (score > 59/72)
    dos-header (size > 64 bytes)
    dos-stub (size > 152 bytes)
    rich-header (tooling > Visual Studio 6.0)
    file-header (executable > 32-bit)
    optional-header (subsystem > GUI)
    directories (count > 2)
    sections (characteristics > self-modifying)
    libraries (flag > 1)
    imports (flag > 2)
    exports (n/a)
    thread-local-storage (n/a)
    .NET (n/a)
    resources (language > flag)
    strings (wait...)
    debug (n/a)
    manifest (n/a)
    version (n/a)
    certificate (n/a)
```

| property | value |
|---|---|
| file | |
| file > sha256 | F09FFE74770A7229DDEF667BC95FA73I |
| file > first 32 bytes (hex) | 4D 5A 90 00 03 00 00 00 04 00 00 00 FF |
| file > first 32 bytes (text) | MZ...............................................@........... |
| file > info | size: 43520 bytes, entropy: 5.565 |
| file > type | executable, 32-bit, GUI |
| file > version | n/a |
| file > description | n/a |
| entry-point > first 32 bytes (hex) | 4D 5A 90 00 03 00 00 00 04 00 00 00 FF |
| entry-point > location | 0x00012790 |
| file > signature | Microsoft Linker 6.0 |
| | |
| stamps | |
| stamp > compiler | Mon May 07 12:58:10 2007 (UTC) |
| stamp > debug | n/a |
| stamp > resource | n/a |
| stamp > import | n/a |
| stamp > export | n/a |
| | |
| names | |



HxD - [C:\Users\Ahtisham\Downloads\malware-sample-2\malware-sample-2\malware-sample\financials-xl...

16 | Windows (ANSI) | hex

financials-xls.exe

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A
00000000  4D 5A 90 00 03 00 00 00 04 00 00
00000010  B8 00 00 00 00 00 00 00 40 00 00
00000020  00 00 00 00 00 00 00 00 00 00 00
00000030  00 00 00 00 00 00 00 00 00 00 00
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01
00000050  69 73 20 70 72 6F 67 72 61 6D 20
00000060  74 20 62 65 20 72 75 6E 20 69 6E
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00
00000080  16 C3 B3 16 52 A2 DD 45 52 A2 DD
00000090  BA BD D7 45 4A A2 DD 45 D1 BE D3
000000A0  52 A2 DD 45 57 A2 DD 45 30 BD CE
000000B0  52 A2 DC 45 07 A2 DD 45 BA BD D6
000000C0  EA A4 DB 45 53 A2 DD 45 52 69 63
000000D0  00 00 00 00 00 00 00 00 50 45 00
000000E0  62 22 3F 46 00 00 00 00 00 00 00
000000F0  0B 01 06 00 00 40 00 00 00 70 00
00000100  90 27 01 00 00 F0 00 00 00 30 01
00000110  00 10 00 00 00 02 00 00 04 00 00
00000120  04 00 00 00 00 00 00 00 00 A0 01
00000130  00 00 00 00 02 00 00 00 00 00 10
00000140  00 00 10 00 00 10 00 00 00 00 00
```

Special editors

Data inspector

| | | |
|---|---|---|
| Binary (8 bit) | | 01001101 |
| Int8 | go to: | 77 |
| UInt8 | go to: | 77 |
| Int16 | go to: | 23117 |
| UInt16 | go to: | 23117 |
| Int24 | go to: | -7316915 |
| UInt24 | go to: | 9460301 |
| Int32 | go to: | 9460301 |
| UInt32 | go to: | 9460301 |
| Int64 | go to: | 12894362189 |
| UInt64 | go to: | 12894362189 |
| LEB128 | go to: | -51 |
| ULEB128 | go to: | 77 |

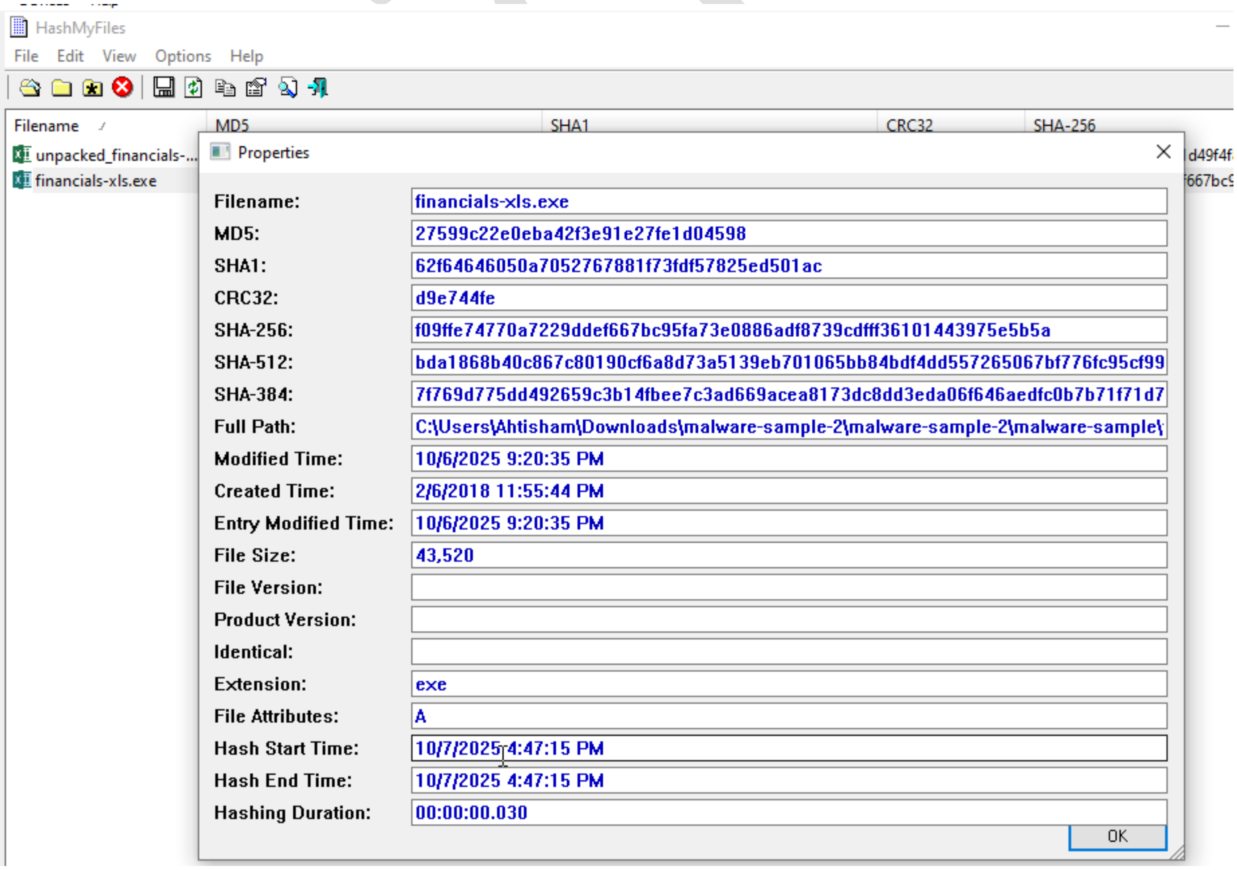
Byte order

● Little endian ○ Big endian

□ Hexadecimal basis (for integral numbers)

Offset(h): 0 Overwri

## Hashes using hashmyfiles of upx-packed sample:

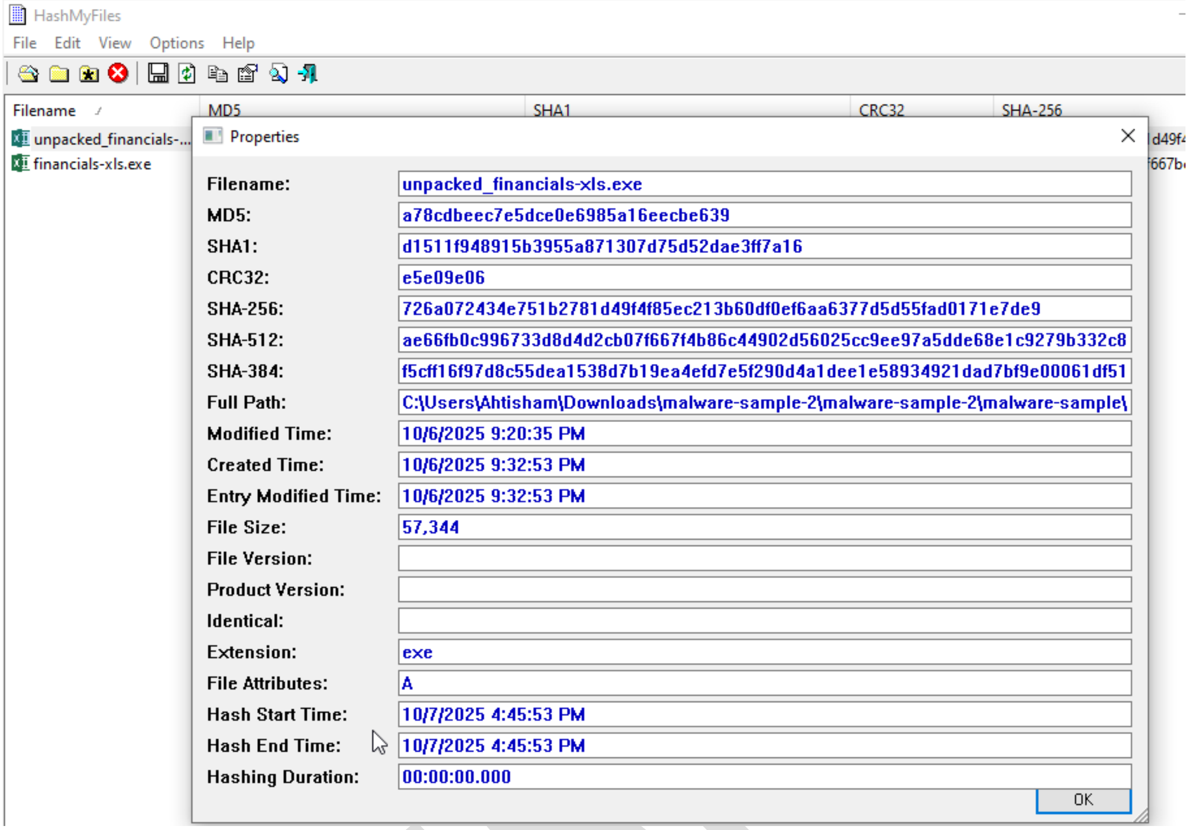


Properties

| | |
|---|---|
| Filename: | financials-xls.exe |
| MD5: | 27599c22e0eba42f3e91e27fe1d04598 |
| SHA1: | 62f64646050a7052767881f73fdf57825ed501ac |
| CRC32: | d9e744fe |
| SHA-256: | f09ffe74770a7229ddef667bc95fa73e0886adf8739cdfff36101443975e5b5a |
| SHA-512: | bda1868b40c867c80190cf6a8d73a5139eb701065bb84bdf4dd557265067bf776fc95cf99 |
| SHA-384: | 7f769d775dd492659c3b14fbee7c3ad669acea8173dc8dd3eda06f646aedfc0b7b71f71d7 |
| Full Path: | C:\Users\Ahtisham\Downloads\malware-sample-2\malware-sample-2\malware-sample\ |
| Modified Time: | 10/6/2025 9:20:35 PM |
| Created Time: | 2/6/2018 11:55:44 PM |
| Entry Modified Time: | 10/6/2025 9:20:35 PM |
| File Size: | 43,520 |
| File Version: | |
| Product Version: | |
| Identical: | |
| Extension: | exe |
| File Attributes: | A |
| Hash Start Time: | 10/7/2025 4:47:15 PM |
| Hash End Time: | 10/7/2025 4:47:15 PM |
| Hashing Duration: | 00:00:00.030 |

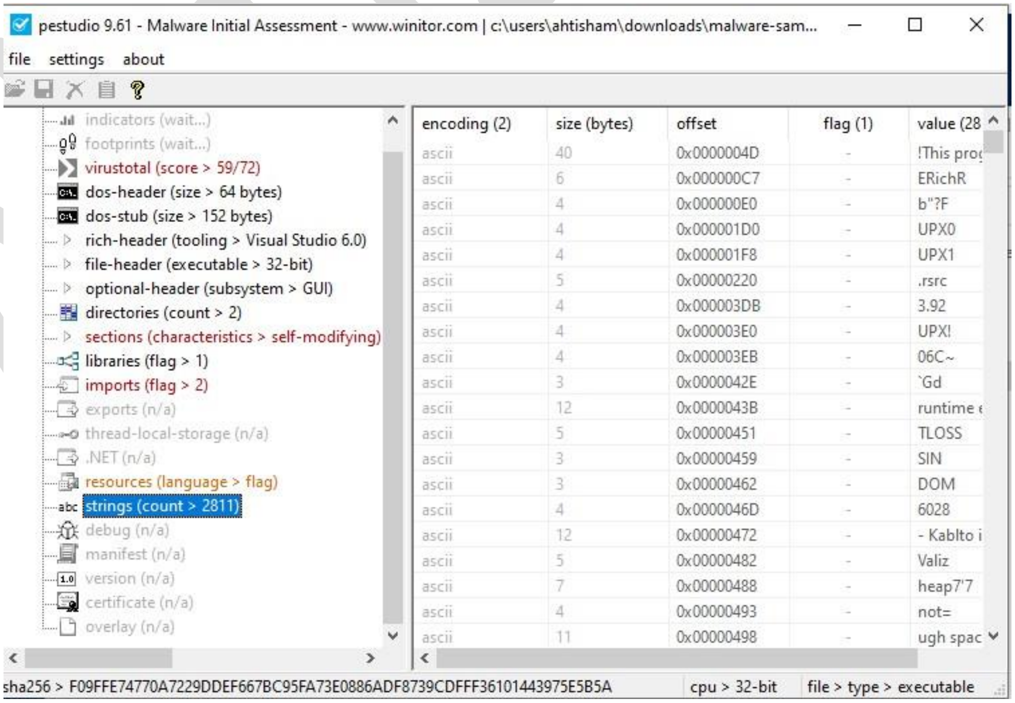
OK

## Hashing of unpacked sample:



| | |
|---|---|
| Filename: | unpacked_financials-xls.exe |
| MD5: | a78cdbeec7e5dce0e6985a16eecbe639 |
| SHA1: | d1511f948915b3955a871307d75d52dae3ff7a16 |
| CRC32: | e5e09e06 |
| SHA-256: | 726a072434e751b2781d49f4f85ec213b60df0ef6aa6377d5d55fad0171e7de9 |
| SHA-512: | ae66fb0c996733d8d4d2cb07f667f4b86c44902d56025cc9ee97a5dde68e1c9279b332c8 |
| SHA-384: | f5cff16f97d8c55dea1538d7b19ea4efd7e5f290d4a1dee1e58934921dad7bf9e00061df51 |
| Full Path: | C:\Users\Ahtisham\Downloads\malware-sample-2\malware-sample-2\malware-sample\ |
| Modified Time: | 10/6/2025 9:20:35 PM |
| Created Time: | 10/6/2025 9:32:53 PM |
| Entry Modified Time: | 10/6/2025 9:32:53 PM |
| File Size: | 57,344 |
| File Version: | |
| Product Version: | |
| Identical: | |
| Extension: | exe |
| File Attributes: | A |
| Hash Start Time: | 10/7/2025 4:45:53 PM |
| Hash End Time: | 10/7/2025 4:45:53 PM |
| Hashing Duration: | 00:00:00.000 |

## String analysis using pestudio:

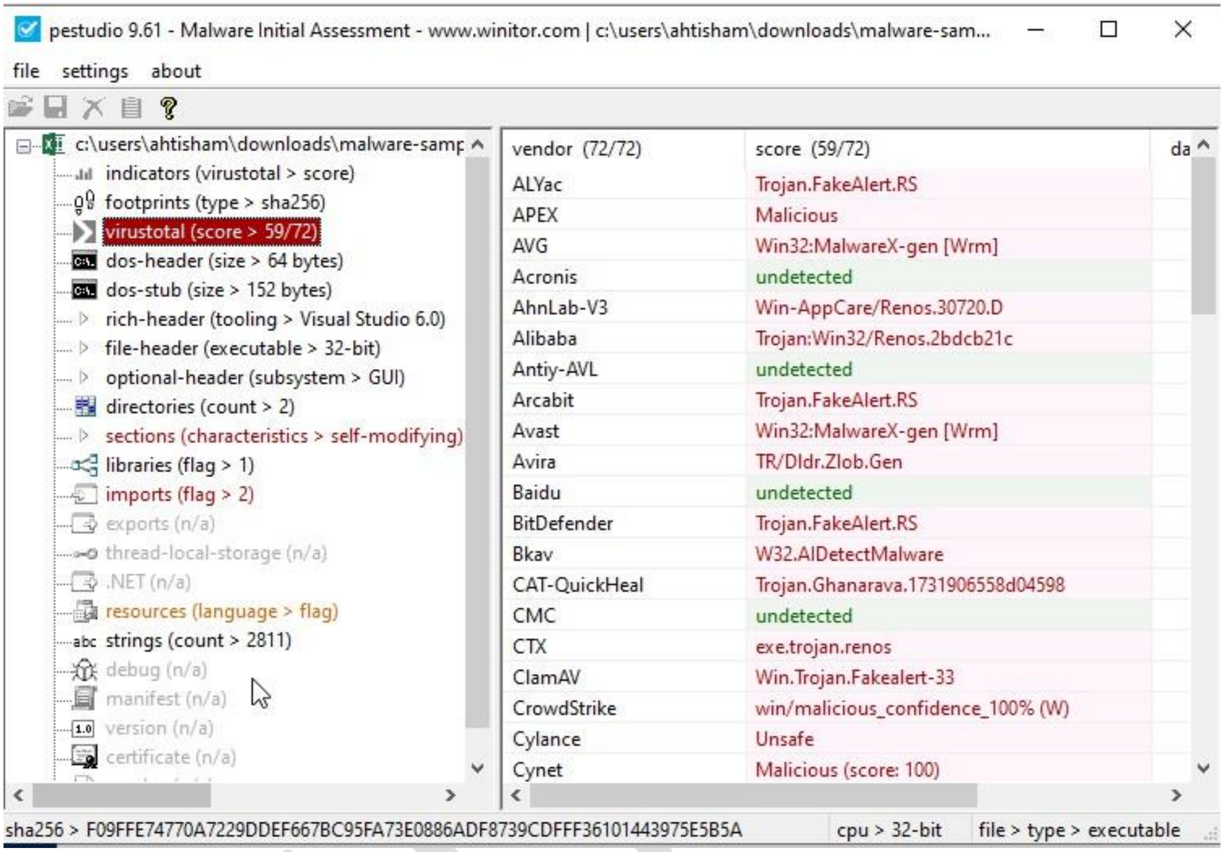

pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\ahtisham\downloads\malware-sam...
file settings about

- indicators (wait...)
- footprints (wait...)
- virustotal (score > 59/72)
- dos-header (size > 64 bytes)
- dos-stub (size > 152 bytes)
- rich-header (tooling > Visual Studio 6.0)
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 2)
- sections (characteristics > self-modifying)
- libraries (flag > 1)
- imports (flag > 2)
- exports (n/a)
- thread-local-storage (n/a)
- .NET (n/a)
- resources (language > flag)
- strings (count > 2811)
- debug (n/a)
- manifest (n/a)
- version (n/a)
- certificate (n/a)
- overlay (n/a)

| encoding (2) | size (bytes) | offset | flag (1) | value (28 |
|---|---|---|---|---|
| ascii | 40 | 0x0000004D | - | !This proc |
| ascii | 6 | 0x000000C7 | - | ERichR |
| ascii | 4 | 0x000000E0 | - | b"?F |
| ascii | 4 | 0x000001D0 | - | UPX0 |
| ascii | 4 | 0x000001F8 | - | UPX1 |
| ascii | 5 | 0x00000220 | - | .rsrc |
| ascii | 4 | 0x000003DB | - | 3.92 |
| ascii | 4 | 0x000003E0 | - | UPX! |
| ascii | 4 | 0x000003EB | - | 06C~ |
| ascii | 3 | 0x0000042E | - | `Gd |
| ascii | 12 | 0x0000043B | - | runtime e |
| ascii | 5 | 0x00000451 | - | TLOSS |
| ascii | 3 | 0x00000459 | - | SIN |
| ascii | 3 | 0x00000462 | - | DOM |
| ascii | 4 | 0x0000046D | - | 6028 |
| ascii | 12 | 0x00000472 | - | - Kablto i |
| ascii | 5 | 0x00000482 | - | Valiz |
| ascii | 7 | 0x00000488 | - | heap7'7 |
| ascii | 4 | 0x00000493 | - | not= |
| ascii | 11 | 0x00000498 | - | ugh spac |

sha256 > F09FFE74770A7229DDEF667BC95FA73E0886ADF8739CDFFF36101443975E5B5A cpu > 32-bit file > type > executable

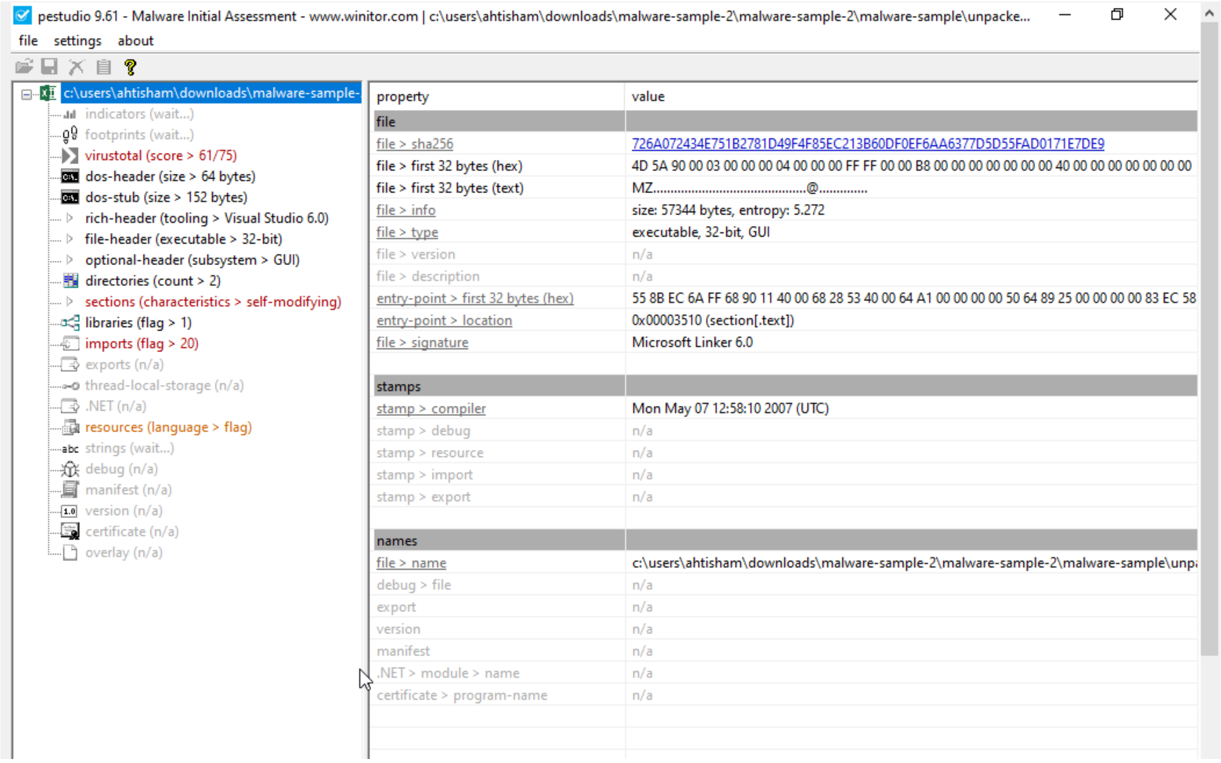
**Score on virus total of packed sample: tool ---->pestudio**


pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\ahtisham\downloads\malware-sam...
file settings about

c:\users\ahtisham\downloads\malware-samp
- indicators (virustotal > score)
- footprints (type > sha256)
- virustotal (score > 59/72)
- dos-header (size > 64 bytes)
- dos-stub (size > 152 bytes)
- rich-header (tooling > Visual Studio 6.0)
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 2)
- sections (characteristics > self-modifying)
- libraries (flag > 1)
- imports (flag > 2)
- exports (n/a)
- thread-local-storage (n/a)
- .NET (n/a)
- resources (language > flag)
- strings (count > 2811)
- debug (n/a)
- manifest (n/a)
- version (n/a)
- certificate (n/a)

| vendor (72/72) | score (59/72) | da |
|---|---|---|
| ALYac | Trojan.FakeAlert.RS | |
| APEX | Malicious | |
| AVG | Win32:MalwareX-gen [Wrm] | |
| Acronis | undetected | |
| AhnLab-V3 | Win-AppCare/Renos.30720.D | |
| Alibaba | Trojan:Win32/Renos.2bdcb21c | |
| Antiy-AVL | undetected | |
| Arcabit | Trojan.FakeAlert.RS | |
| Avast | Win32:MalwareX-gen [Wrm] | |
| Avira | TR/Dldr.Zlob.Gen | |
| Baidu | undetected | |
| BitDefender | Trojan.FakeAlert.RS | |
| Bkav | W32.AIDetectMalware | |
| CAT-QuickHeal | Trojan.Ghanarava.1731906558d04598 | |
| CMC | undetected | |
| CTX | exe.trojan.renos | |
| ClamAV | Win.Trojan.Fakealert-33 | |
| CrowdStrike | win/malicious_confidence_100% (W) | |
| Cylance | Unsafe | |
| Cynet | Malicious (score: 100) | |

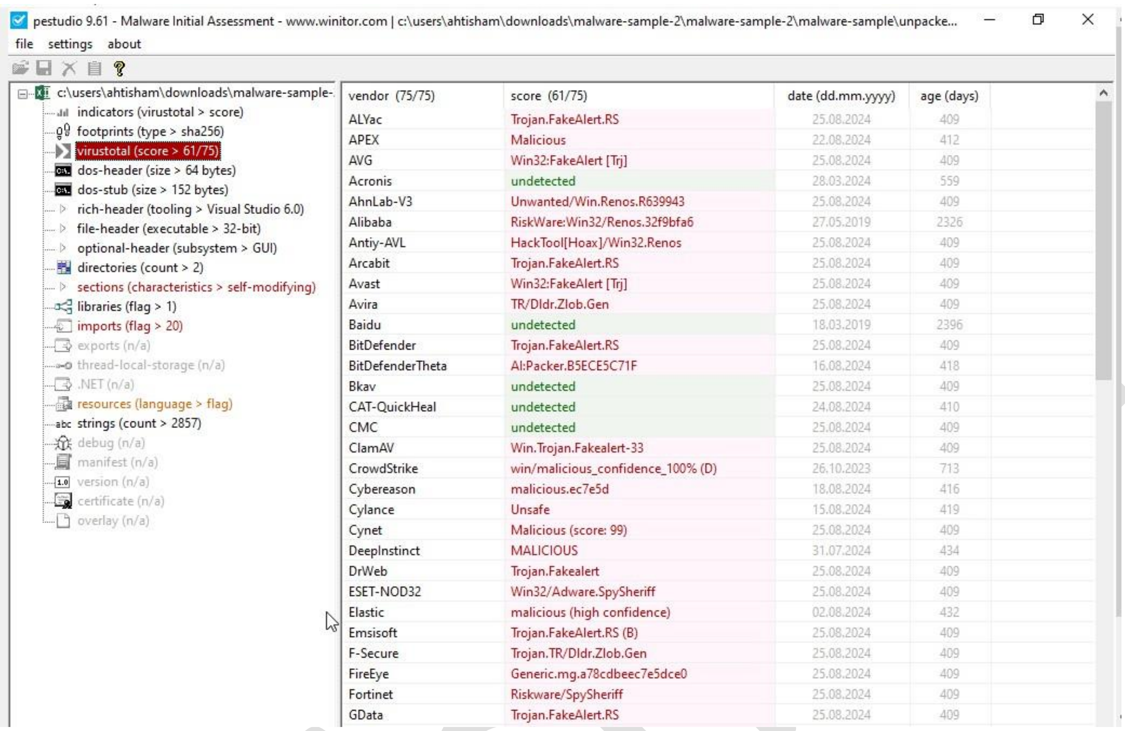
sha256 > F09FFE74770A7229DDEF667BC95FA73E0886ADF8739CDFFF36101443975E5B5A cpu > 32-bit file > type > executable


pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\ahtisham\downloads\malware-sample-2\malware-sample-2\malware-sample\unpacke...
file settings about

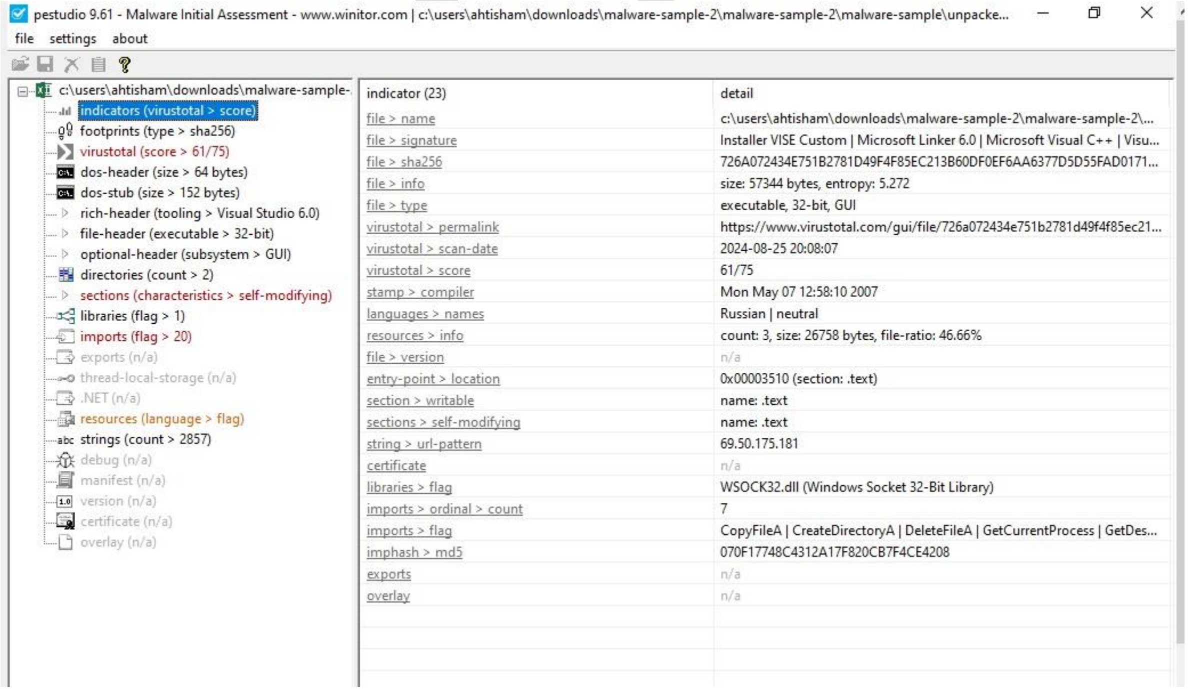
c:\users\ahtisham\downloads\malware-sample-
- indicators (wait...)
- footprints (wait...)
- virustotal (score > 61/75)
- dos-header (size > 64 bytes)
- dos-stub (size > 152 bytes)
- rich-header (tooling > Visual Studio 6.0)
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 2)
- sections (characteristics > self-modifying)
- libraries (flag > 1)
- imports (flag > 20)
- exports (n/a)
- thread-local-storage (n/a)
- .NET (n/a)
- resources (language > flag)
- strings (wait...)
- debug (n/a)
- manifest (n/a)
- version (n/a)
- certificate (n/a)
- overlay (n/a)

| property | value |
|---|---|
| file | |
| file > sha256 | 726A072434E751B2781D49F4F85EC213B60DF0EF6AA6377D5D55FAD0171E7DE9 |
| file > first 32 bytes (hex) | 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 |
| file > first 32 bytes (text) | MZ.........................................@............. |
| file > info | size: 57344 bytes, entropy: 5.272 |
| file > type | executable, 32-bit, GUI |
| file > version | n/a |
| file > description | n/a |
| entry-point > first 32 bytes (hex) | 55 8B EC 6A FF 68 90 11 40 00 68 28 53 40 00 64 A1 00 00 00 00 50 64 89 25 00 00 00 00 83 EC 58 |
| entry-point > location | 0x00003510 (section[.text]) |
| file > signature | Microsoft Linker 6.0 |
| | |
| stamps | |
| stamp > compiler | Mon May 07 12:58:10 2007 (UTC) |
| stamp > debug | n/a |
| stamp > resource | n/a |
| stamp > import | n/a |
| stamp > export | n/a |
| | |
| names | |
| file > name | c:\users\ahtisham\downloads\malware-sample-2\malware-sample-2\malware-sample\unpa |
| debug > file | n/a |
| export | n/a |
| version | n/a |
| manifest | n/a |
| .NET > module > name | n/a |
| certificate > program-name | n/a |

## Virus total Score of unpacked malware:

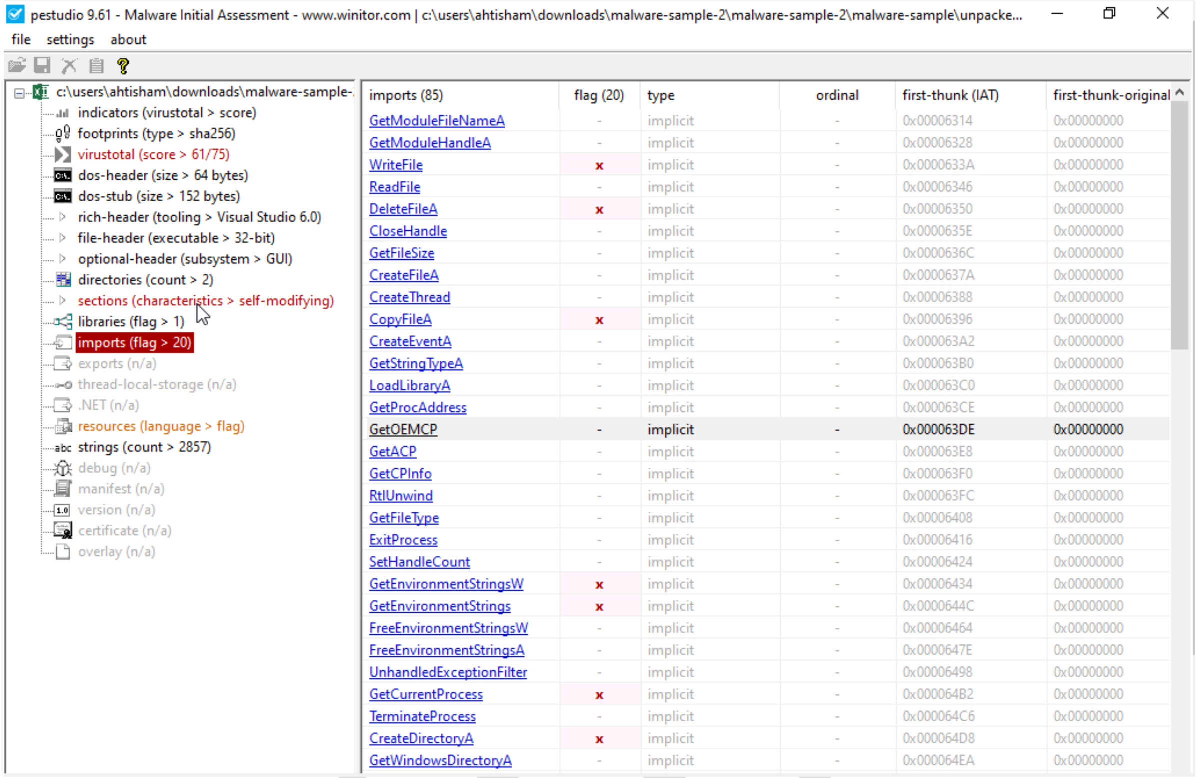

pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\ahtisham\downloads\malware-sample-2\malware-sample-2\malware-sample\unpacke...
file
settings
about
c:\users\ahtisham\downloads\malware-sample-
indicators (virustotal > score)
footprints (type > sha256)
virustotal (score > 61/75)
dos-header (size > 64 bytes)
dos-stub (size > 152 bytes)
rich-header (tooling > Visual Studio 6.0)
file-header (executable > 32-bit)
optional-header (subsystem > GUI)
directories (count > 2)
sections (characteristics > self-modifying)
libraries (flag > 1)
imports (flag > 20)
exports (n/a)
thread-local-storage (n/a)
.NET (n/a)
resources (language > flag)
strings (count > 2857)
debug (n/a)
manifest (n/a)
version (n/a)
certificate (n/a)
overlay (n/a)

| vendor (75/75) | score (61/75) | date (dd.mm.yyyy) | age (days) |
|---|---|---|---|
| ALYac | Trojan.FakeAlert.RS | 25.08.2024 | 409 |
| APEX | Malicious | 22.08.2024 | 412 |
| AVG | Win32:FakeAlert [Trj] | 25.08.2024 | 409 |
| Acronis | undetected | 28.03.2024 | 559 |
| AhnLab-V3 | Unwanted/Win.Renos.R639943 | 25.08.2024 | 409 |
| Alibaba | RiskWare:Win32/Renos.32f9bfa6 | 27.05.2019 | 2326 |
| Antiy-AVL | HackTool[Hoax]/Win32.Renos | 25.08.2024 | 409 |
| Arcabit | Trojan.FakeAlert.RS | 25.08.2024 | 409 |
| Avast | Win32:FakeAlert [Trj] | 25.08.2024 | 409 |
| Avira | TR/Dldr.Zlob.Gen | 25.08.2024 | 409 |
| Baidu | undetected | 18.03.2019 | 2396 |
| BitDefender | Trojan.FakeAlert.RS | 25.08.2024 | 409 |
| BitDefenderTheta | AI:Packer.B5ECE5C71F | 16.08.2024 | 418 |
| Bkav | undetected | 25.08.2024 | 409 |
| CAT-QuickHeal | undetected | 24.08.2024 | 410 |
| CMC | undetected | 25.08.2024 | 409 |
| ClamAV | Win.Trojan.Fakealert-33 | 25.08.2024 | 409 |
| CrowdStrike | win/malicious_confidence_100% (D) | 26.10.2023 | 713 |
| Cybereason | malicious.ec7e5d | 18.08.2024 | 416 |
| Cylance | Unsafe | 15.08.2024 | 419 |
| Cynet | Malicious (score: 99) | 25.08.2024 | 409 |
| DeepInstinct | MALICIOUS | 31.07.2024 | 434 |
| DrWeb | Trojan.Fakealert | 25.08.2024 | 409 |
| ESET-NOD32 | Win32/Adware.SpySheriff | 25.08.2024 | 409 |
| Elastic | malicious (high confidence) | 02.08.2024 | 432 |
| Emsisoft | Trojan.FakeAlert.RS (B) | 25.08.2024 | 409 |
| F-Secure | Trojan.TR/Dldr.Zlob.Gen | 25.08.2024 | 409 |
| FireEye | Generic.mg.a78cdbeec7e5dce0 | 25.08.2024 | 409 |
| Fortinet | Riskware/SpySheriff | 25.08.2024 | 409 |
| GData | Trojan.FakeAlert.RS | 25.08.2024 | 409 |


pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\ahtisham\downloads\malware-sample-2\malware-sample-2\malware-sample\unpacke...
file
settings
about
c:\users\ahtisham\downloads\malware-sample-
indicators (virustotal > score)
footprints (type > sha256)
virustotal (score > 61/75)
dos-header (size > 64 bytes)
dos-stub (size > 152 bytes)
rich-header (tooling > Visual Studio 6.0)
file-header (executable > 32-bit)
optional-header (subsystem > GUI)
directories (count > 2)
sections (characteristics > self-modifying)
libraries (flag > 1)
imports (flag > 20)
exports (n/a)
thread-local-storage (n/a)
.NET (n/a)
resources (language > flag)
strings (count > 2857)
debug (n/a)
manifest (n/a)
version (n/a)
certificate (n/a)
overlay (n/a)

| indicator (23) | detail |
|---|---|
| file > name | c:\users\ahtisham\downloads\malware-sample-2\malware-sample-2\... |
| file > signature | Installer VISE Custom \| Microsoft Linker 6.0 \| Microsoft Visual C++ \| Visu... |
| file > sha256 | 726A072434E751B2781D49F4F85EC213B60DF0EF6AA6377D5D55FAD0171... |
| file > info | size: 57344 bytes, entropy: 5.272 |
| file > type | executable, 32-bit, GUI |
| virustotal > permalink | https://www.virustotal.com/gui/file/726a072434e751b2781d49f4f85ec21... |
| virustotal > scan-date | 2024-08-25 20:08:07 |
| virustotal > score | 61/75 |
| stamp > compiler | Mon May 07 12:58:10 2007 |
| languages > names | Russian \| neutral |
| resources > info | count: 3, size: 26758 bytes, file-ratio: 46.66% |
| file > version | n/a |
| entry-point > location | 0x00003510 (section: .text) |
| section > writable | name: .text |
| sections > self-modifying | name: .text |
| string > url-pattern | 69.50.175.181 |
| certificate | n/a |
| libraries > flag | WSOCK32.dll (Windows Socket 32-Bit Library) |
| imports > ordinal > count | 7 |
| imports > flag | CopyFileA \| CreateDirectoryA \| DeleteFileA \| GetCurrentProcess \| GetDes... |
| imphash > md5 | 070F17748C4312A17F820CB7F4CE4208 |
| exports | n/a |
| overlay | n/a |

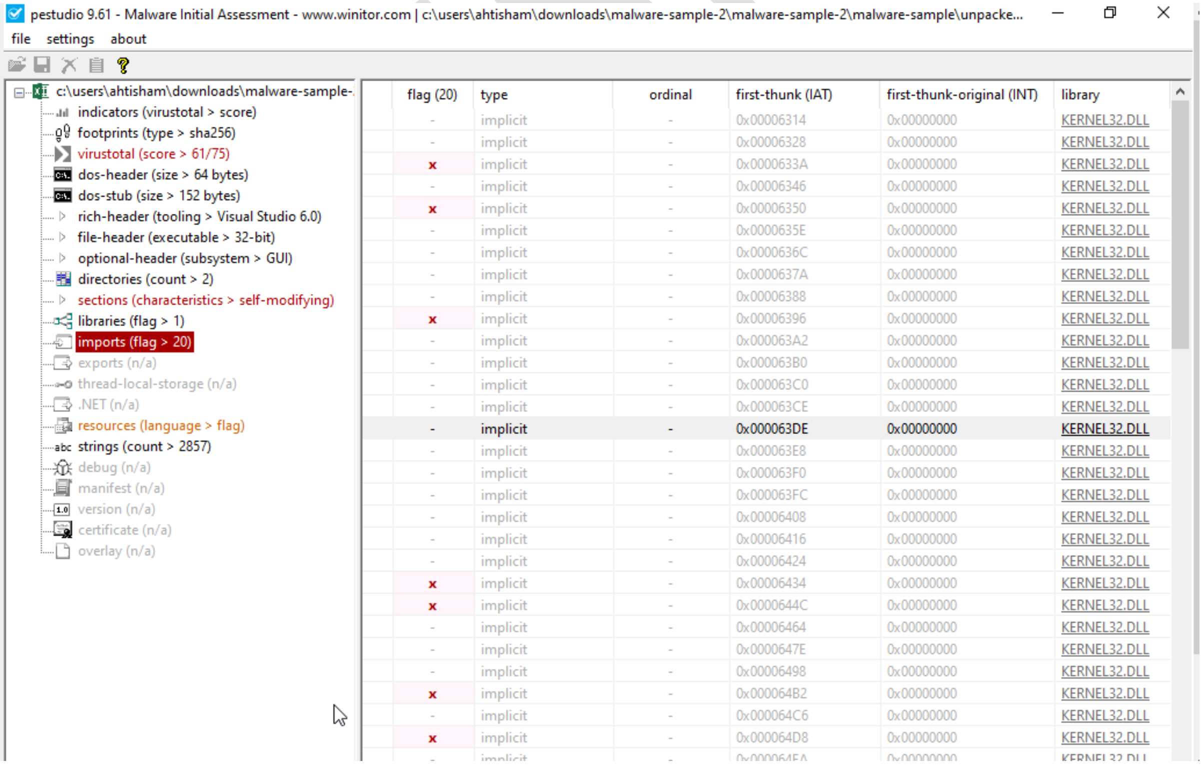
## Imports:



pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\ahtisham\downloads\malware-sample-2\malware-sample-2\malware-sample\unpacke...

c:\users\ahtisham\downloads\malware-sample-
- indicators (virustotal > score)
- footprints (type > sha256)
- virustotal (score > 61/75)
- dos-header (size > 64 bytes)
- dos-stub (size > 152 bytes)
- rich-header (tooling > Visual Studio 6.0)
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 2)
- sections (characteristics > self-modifying)
- libraries (flag > 1)
- imports (flag > 20)
- exports (n/a)
- thread-local-storage (n/a)
- .NET (n/a)
- resources (language > flag)
- strings (count > 2857)
- debug (n/a)
- manifest (n/a)
- version (n/a)
- certificate (n/a)
- overlay (n/a)

| imports (85) | flag (20) | type | ordinal | first-thunk (IAT) | first-thunk-original |
|---|---|---|---|---|---|
| GetModuleFileNameA | - | implicit | - | 0x00006314 | 0x00000000 |
| GetModuleHandleA | - | implicit | - | 0x00006328 | 0x00000000 |
| WriteFile | x | implicit | - | 0x0000633A | 0x00000000 |
| ReadFile | - | implicit | - | 0x00006346 | 0x00000000 |
| DeleteFileA | x | implicit | - | 0x00006350 | 0x00000000 |
| CloseHandle | - | implicit | - | 0x0000635E | 0x00000000 |
| GetFileSize | - | implicit | - | 0x0000636C | 0x00000000 |
| CreateFileA | - | implicit | - | 0x0000637A | 0x00000000 |
| CreateThread | - | implicit | - | 0x00006388 | 0x00000000 |
| CopyFileA | x | implicit | - | 0x00006396 | 0x00000000 |
| CreateEventA | - | implicit | - | 0x000063A2 | 0x00000000 |
| GetStringTypeA | - | implicit | - | 0x000063B0 | 0x00000000 |
| LoadLibraryA | - | implicit | - | 0x000063C0 | 0x00000000 |
| GetProcAddress | - | implicit | - | 0x000063CE | 0x00000000 |
| GetOEMCP | - | implicit | - | 0x000063DE | 0x00000000 |
| GetACP | - | implicit | - | 0x000063E8 | 0x00000000 |
| GetCPInfo | - | implicit | - | 0x000063F0 | 0x00000000 |
| RtlUnwind | - | implicit | - | 0x000063FC | 0x00000000 |
| GetFileType | - | implicit | - | 0x00006408 | 0x00000000 |
| ExitProcess | - | implicit | - | 0x00006416 | 0x00000000 |
| SetHandleCount | - | implicit | - | 0x00006424 | 0x00000000 |
| GetEnvironmentStringsW | x | implicit | - | 0x00006434 | 0x00000000 |
| GetEnvironmentStrings | x | implicit | - | 0x0000644C | 0x00000000 |
| FreeEnvironmentStringsW | - | implicit | - | 0x00006464 | 0x00000000 |
| FreeEnvironmentStringsA | - | implicit | - | 0x0000647E | 0x00000000 |
| UnhandledExceptionFilter | - | implicit | - | 0x00006498 | 0x00000000 |
| GetCurrentProcess | x | implicit | - | 0x000064B2 | 0x00000000 |
| TerminateProcess | - | implicit | - | 0x000064C6 | 0x00000000 |
| CreateDirectoryA | x | implicit | - | 0x000064D8 | 0x00000000 |
| GetWindowsDirectoryA | - | implicit | - | 0x000064EA | 0x00000000 |

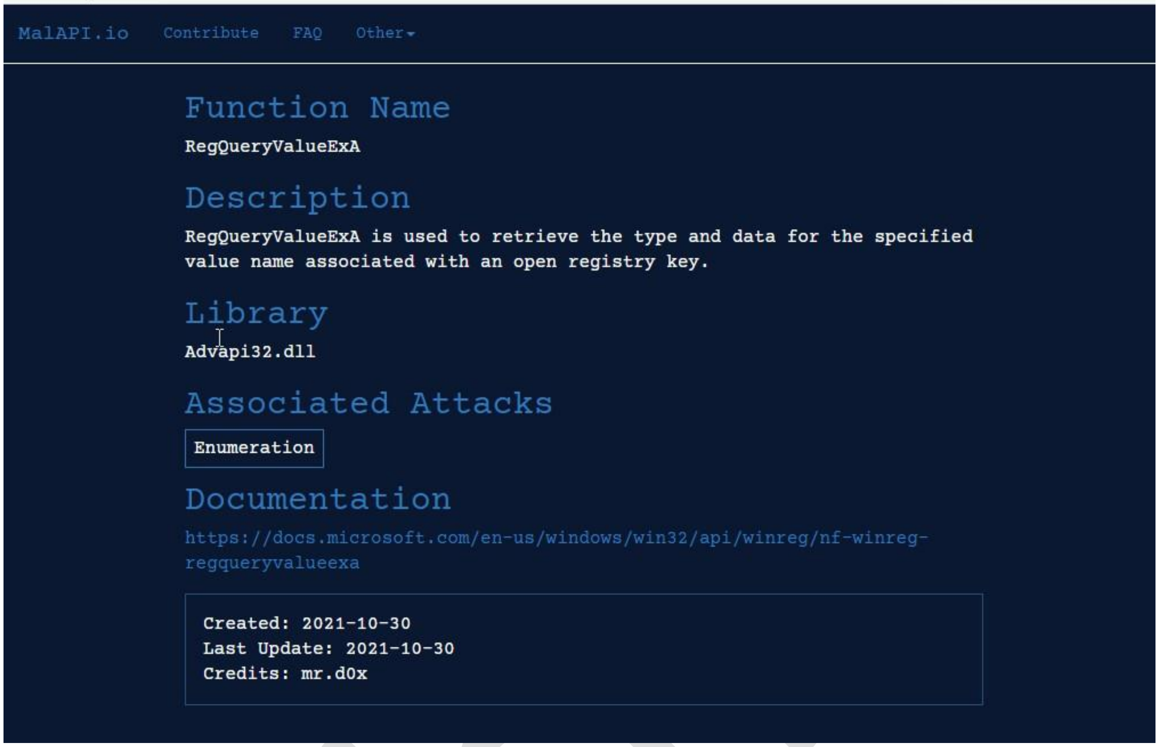


pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\ahtisham\downloads\malware-sample-2\malware-sample-2\malware-sample\unpacke...

c:\users\ahtisham\downloads\malware-sample-
- indicators (virustotal > score)
- footprints (type > sha256)
- virustotal (score > 61/75)
- dos-header (size > 64 bytes)
- dos-stub (size > 152 bytes)
- rich-header (tooling > Visual Studio 6.0)
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 2)
- sections (characteristics > self-modifying)
- libraries (flag > 1)
- imports (flag > 20)
- exports (n/a)
- thread-local-storage (n/a)
- .NET (n/a)
- resources (language > flag)
- strings (count > 2857)
- debug (n/a)
- manifest (n/a)
- version (n/a)
- certificate (n/a)
- overlay (n/a)

| flag (20) | type | ordinal | first-thunk (IAT) | first-thunk-original (INT) | library |
|---|---|---|---|---|---|
| - | implicit | - | 0x00006314 | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x00006328 | 0x00000000 | KERNEL32.DLL |
| x | implicit | - | 0x0000633A | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x00006346 | 0x00000000 | KERNEL32.DLL |
| x | implicit | - | 0x00006350 | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x0000635E | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x0000636C | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x0000637A | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x00006388 | 0x00000000 | KERNEL32.DLL |
| x | implicit | - | 0x00006396 | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x000063A2 | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x000063B0 | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x000063C0 | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x000063CE | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x000063DE | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x000063E8 | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x000063F0 | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x000063FC | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x00006408 | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x00006416 | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x00006424 | 0x00000000 | KERNEL32.DLL |
| x | implicit | - | 0x00006434 | 0x00000000 | KERNEL32.DLL |
| x | implicit | - | 0x0000644C | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x00006464 | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x0000647E | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x00006498 | 0x00000000 | KERNEL32.DLL |
| x | implicit | - | 0x000064B2 | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x000064C6 | 0x00000000 | KERNEL32.DLL |
| x | implicit | - | 0x000064D8 | 0x00000000 | KERNEL32.DLL |
| - | implicit | - | 0x000064EA | 0x00000000 | KERNEL32.DLL |

## MalAPI.io (Malware's API Analysis Tool):



Function Name

RegQueryValueExA

Description

RegQueryValueExA is used to retrieve the type and data for the specified value name associated with an open registry key.

Library

Advapi32.dll

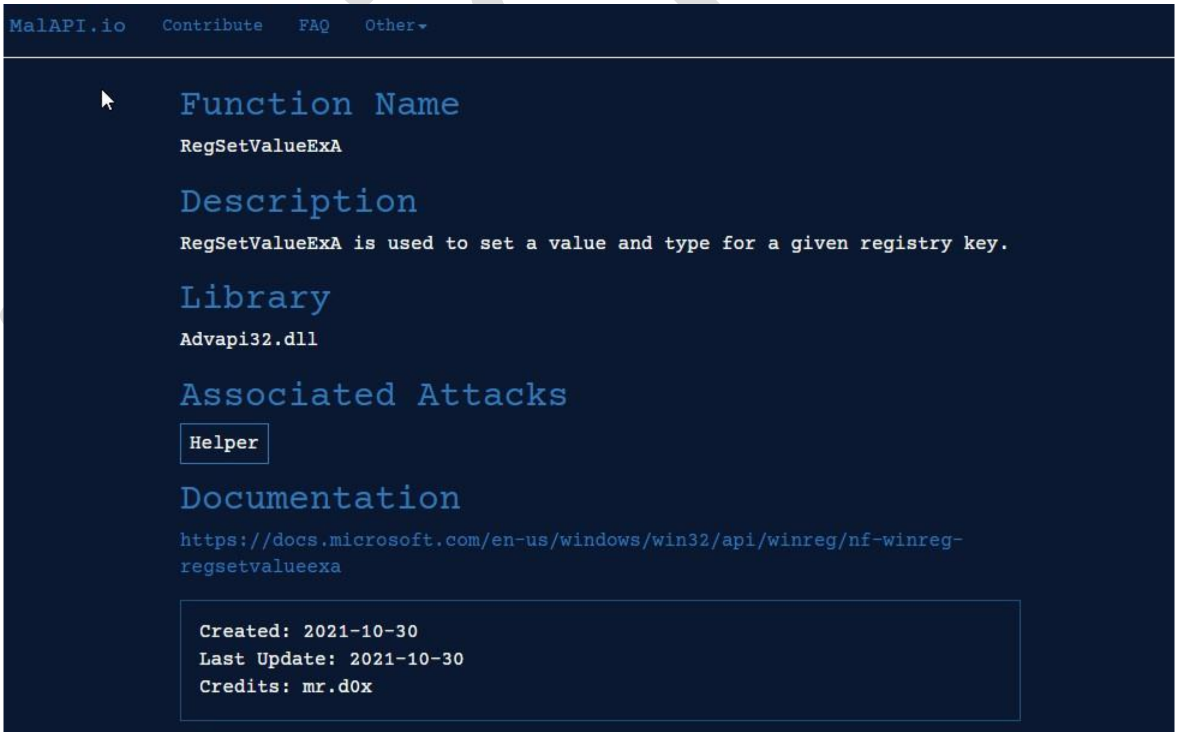
Associated Attacks

Enumeration

Documentation

https://docs.microsoft.com/en-us/windows/win32/api/winreg/nf-winreg-regqueryvalueexa

Created: 2021-10-30
Last Update: 2021-10-30
Credits: mr.d0x



Function Name

RegSetValueExA

Description

RegSetValueExA is used to set a value and type for a given registry key.

Library

Advapi32.dll

Associated Attacks

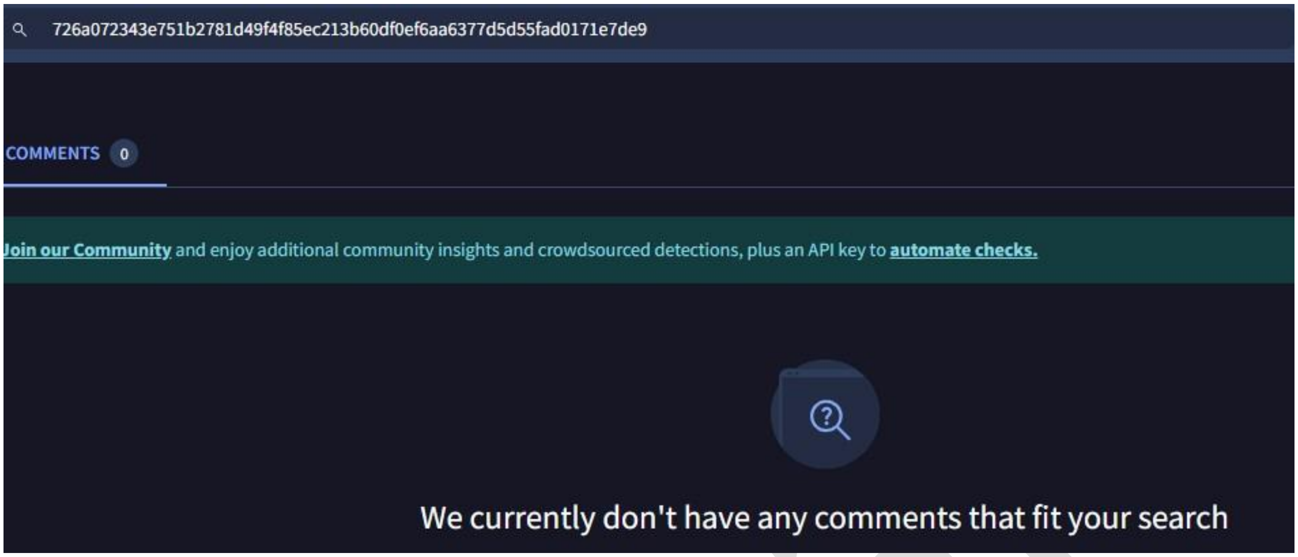
Helper

Documentation

https://docs.microsoft.com/en-us/windows/win32/api/winreg/nf-winreg-regsetvalueexa

Created: 2021-10-30
Last Update: 2021-10-30
Credits: mr.d0x

### MD256 Hash Check Using Virus Total:



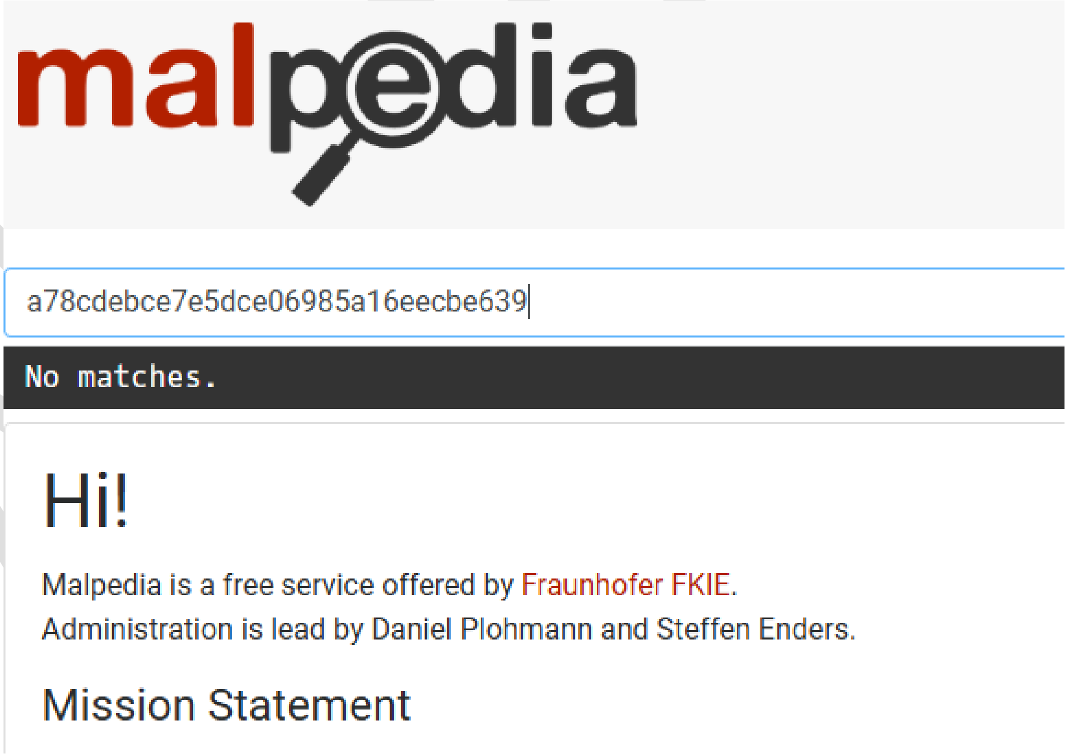
726a072343e751b2781d49f4f85ec213b60df0ef6aa6377d5d55fad0171e7de9

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

We currently don't have any comments that fit your search

### Checking Malware Family Using mapedia:

Using malware’s Hashes, we can easily search malware sample’s family record:



a78cdebce7e5dce06985a16eecbe639

No matches.

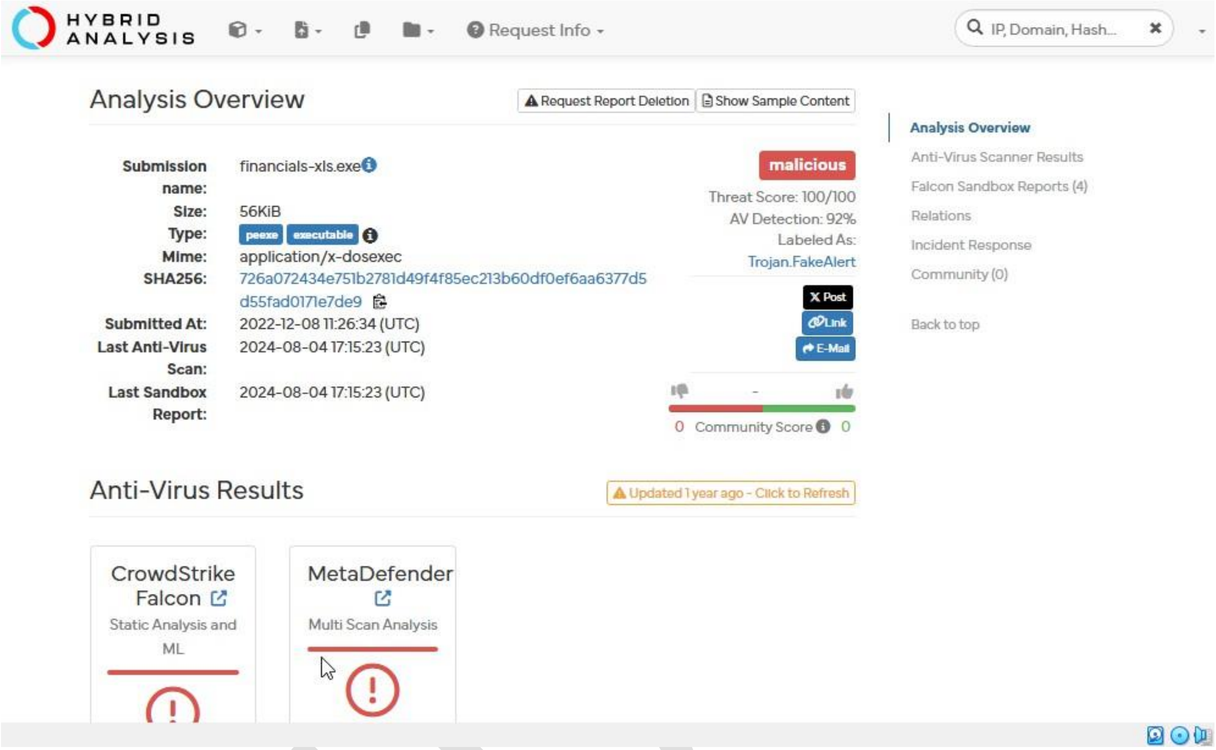
Hi!

Malpedia is a free service offered by Fraunhofer FKIE.
Administration is lead by Daniel Plohmann and Steffen Enders.

Mission Statement

## Uploading malware sample:

Our task was to submit malware sample to MalAPI.io Analyzer but after recent update in MalAPI.io we are unable to upload our malware sample so we have used different tools. given below



Analysis Overview

Submission name: financials-xls.exe

Size: 56KiB

Type: peexe executable

Mime: application/x-dosexec

SHA256: 726a072434e751b2781d49f4f85ec213b60df0ef6aa6377d5d55fad0171e7de9

Submitted At: 2022-12-08 11:26:34 (UTC)

Last Anti-Virus Scan: 2024-08-04 17:15:23 (UTC)

Last Sandbox Report: 2024-08-04 17:15:23 (UTC)

malicious

Threat Score: 100/100

AV Detection: 92%

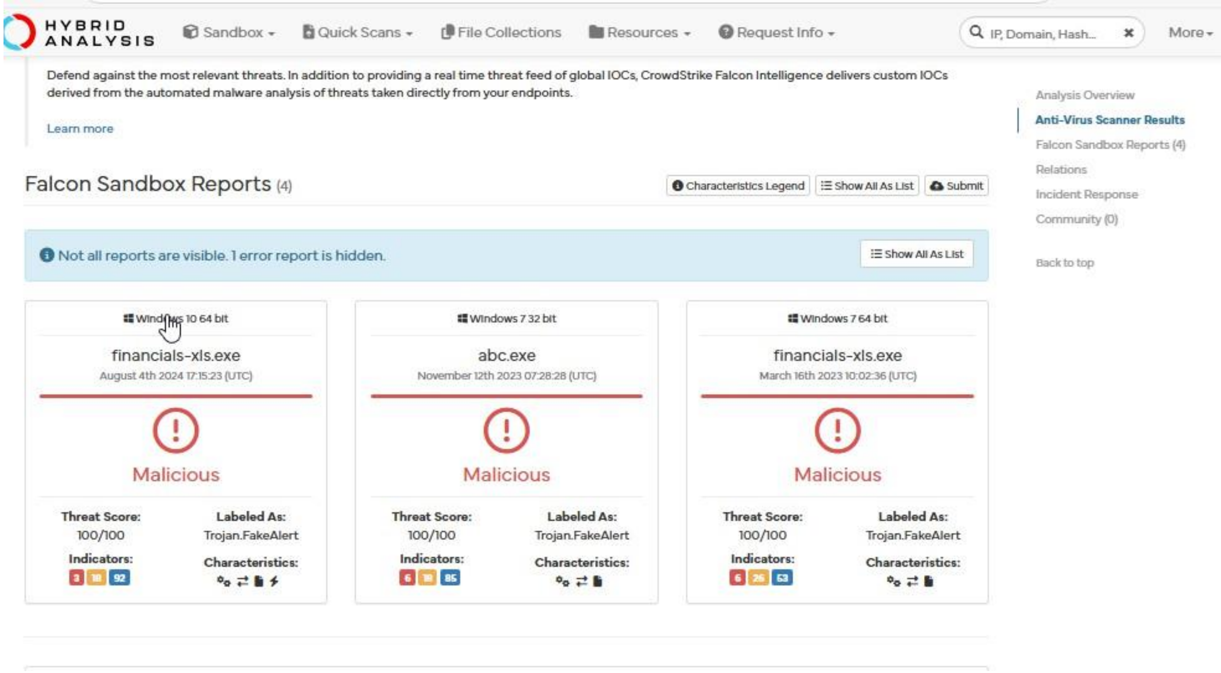
Labeled As: Trojan.FakeAlert

0 Community Score 0

Anti-Virus Results

CrowdStrike Falcon
Static Analysis and ML

MetaDefender
Multi Scan Analysis



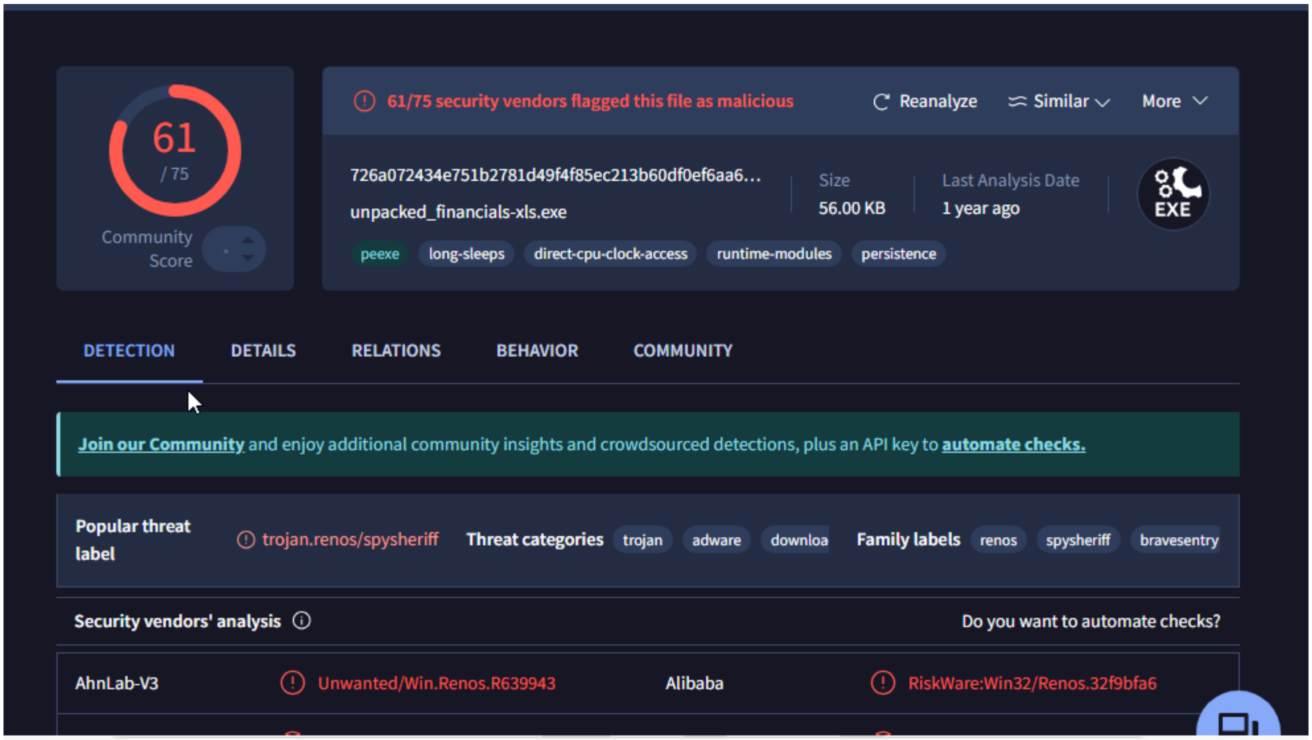
Defend against the most relevant threats. In addition to providing a real time threat feed of global IOCs, CrowdStrike Falcon Intelligence delivers custom IOCs derived from the automated malware analysis of threats taken directly from your endpoints.

Falcon Sandbox Reports (4)

Not all reports are visible. 1 error report is hidden.

| Windows 10 64 bit | Windows 7 32 bit | Windows 7 64 bit |
|---|---|---|
| financials-xls.exe<br>August 4th 2024 17:15:23 (UTC) | abc.exe<br>November 12th 2023 07:28:28 (UTC) | financials-xls.exe<br>March 16th 2023 10:02:36 (UTC) |
| Malicious | Malicious | Malicious |
| Threat Score: 100/100 | Threat Score: 100/100 | Threat Score: 100/100 |
| Labeled As: Trojan.FakeAlert | Labeled As: Trojan.FakeAlert | Labeled As: Trojan.FakeAlert |
| Indicators: 3 18 92 | Indicators: 6 18 85 | Indicators: 6 26 53 |
| Characteristics: | Characteristics: | Characteristics: |

### Uploading malware sample on Virus Total:



61/75 security vendors flagged this file as malicious

726a072434e751b2781d49f4f85ec213b60df0ef6aa6...
unpacked_financials-xls.exe

Size
56.00 KB

Last Analysis Date
1 year ago

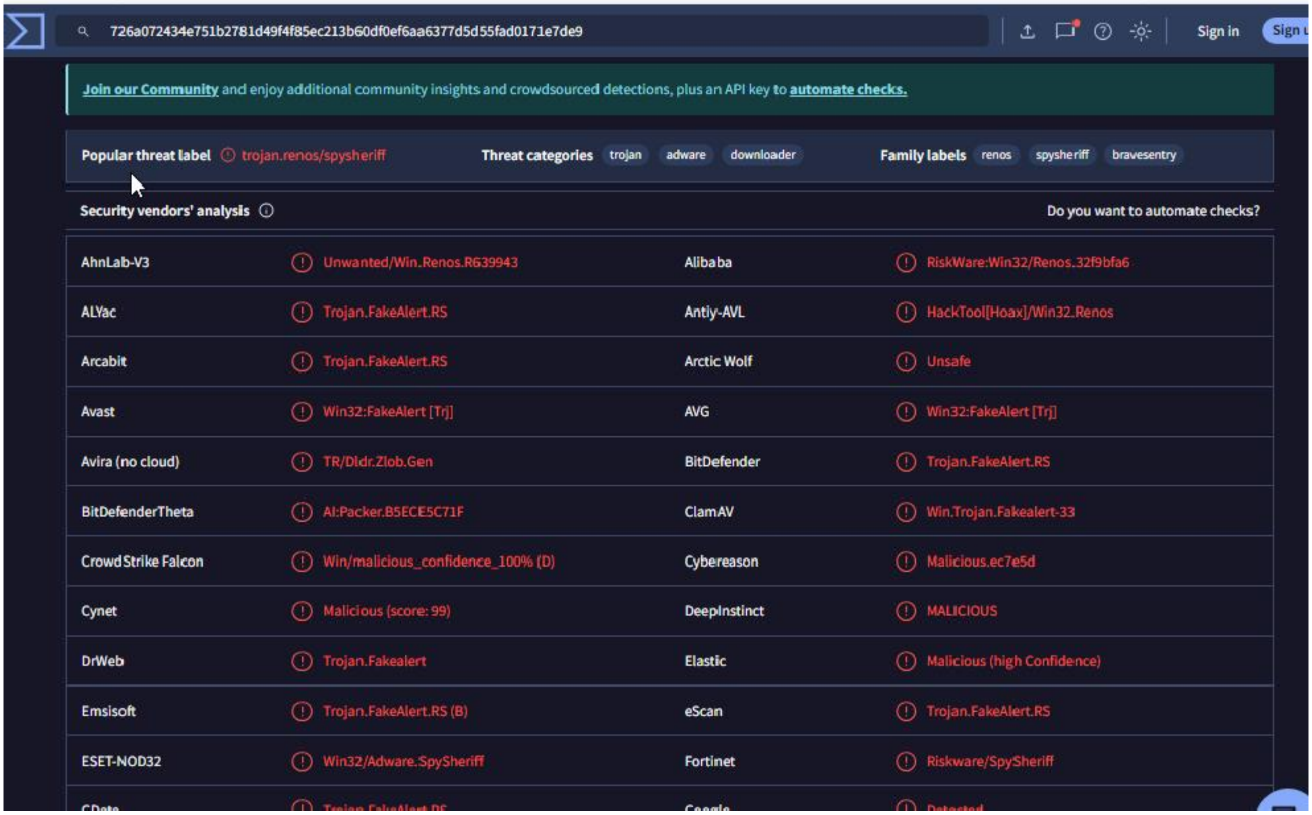
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.renos/spysheriff
Threat categories trojan adware downloa
Family labels renos spysheriff bravesentry

Security vendors' analysis

Do you want to automate checks?

| | | | |
|---|---|---|---|
| AhnLab-V3 | Unwanted/Win.Renos.R639943 | Alibaba | RiskWare:Win32/Renos.32f9bfa6 |



726a072434e751b2781d49f4f85ec213b60df0ef6aa6377d5d55fad0171e7de9

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.renos/spysheriff
Threat categories trojan adware downloader
Family labels renos spysheriff bravesentry

Security vendors' analysis

Do you want to automate checks?

| | | | |
|---|---|---|---|
| AhnLab-V3 | Unwanted/Win.Renos.R639943 | Alibaba | RiskWare:Win32/Renos.32f9bfa6 |
| ALYac | Trojan.FakeAlert.RS | Antiy-AVL | HackTool[Hoax]/Win32.Renos |
| Arcabit | Trojan.FakeAlert.RS | Arctic Wolf | Unsafe |
| Avast | Win32:FakeAlert [Trj] | AVG | Win32:FakeAlert [Trj] |
| Avira (no cloud) | TR/Dldr.Zlob.Gen | BitDefender | Trojan.FakeAlert.RS |
| BitDefenderTheta | AI:Packer.B5ECE5C71F | ClamAV | Win.Trojan.Fakealert-33 |
| CrowdStrike Falcon | Win/malicious_confidence_100% (D) | Cybereason | Malicious.ec7e5d |
| Cynet | Malicious (score: 99) | DeepInstinct | MALICIOUS |
| DrWeb | Trojan.Fakealert | Elastic | Malicious (high Confidence) |
| Emsisoft | Trojan.FakeAlert.RS (B) | eScan | Trojan.FakeAlert.RS |
| ESET-NOD32 | Win32/Adware.SpySheriff | Fortinet | Riskware/SpySheriff |
| CDate | Trojan.FakeAlert.RS | Google | Detected |